#3

PATENT
83308.0001
Express Mail Label No. EL 589 806 213 US

JC928 U.S. PTO 09/726180 11/29/00

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	Art Unit: Not assigned
Masao KASAHARA	Examiner: Not assigned
Serial No: Not assigned	
Filed: November 29, 2000	
For: A CRYPTOSYSTEM USING MULTIVARIABLE POLYNOMIALS	

TRANSMITTAL OF PRIORITY DOCUMENT

Box PATENT APPLICATION
Assistant Commissioner for Patents
Washington, D.C. 20231

Dear Sir:

Enclosed herewith is a certified copy of Japanese patent application No. 2000-066226 which was filed March 10, 2000, from which priority is claimed under 35 U.S.C. § 119 and Rule 55.

Acknowledgment of the priority document(s) is respectfully requested to ensure that the subject information appears on the printed patent.

Respectfully submitted,

HOGAN & HARTSON L.L.P.

Date: November 29, 2000

By: _____
Louis A. Mok
Registration No. 22,585
Attorney for Applicant(s)

500 South Grand Avenue, Suite 1900
Los Angeles, California 90071
Telephone: 213-337-6700
Facsimile: 213-337-6701

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２０００年 ３月１０日

願 番 号
Application Number: 特願２０００－０６６２２６

願 人
Applicant (s): 村田機械株式会社
笠原 正雄

CERTIFIED COPY OF
PRIORITY DOCUMENT

２０００年 ７月２８日

特 許 庁 長 官
Commissioner,
Patent Office 及川耕造

出証番号 出証特２０００－３０６０２６３

【書類名】　特許願
【整理番号】　MF0001
【特記事項】　特許法第３０条第１項の規定の適用を受けようとする特許出願
【あて先】　特許庁長官　殿
【国際特許分類】　H04L　9/00
【発明者】
　【住所又は居所】　大阪府箕面市粟生外院４丁目１５番３号
　【氏名】　笠原　正雄
【特許出願人】
　【識別番号】　000006297
　【氏名又は名称】　村田機械株式会社
【特許出願人】
　【識別番号】　597008636
　【氏名又は名称】　笠原　正雄
【代理人】
　【識別番号】　100086830
　【弁理士】
　【氏名又は名称】　塩入　明
【選任した代理人】
　【識別番号】　100096046
　【弁理士】
　【氏名又は名称】　塩入　みか
【手数料の表示】
　【予納台帳番号】　012047
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1

【物件名】　　要約書　1

【包括委任状番号】　9804018

【プルーフの要否】　　要

【書類名】　明細書

【発明の名称】　復号方法、復号装置、及び復号プログラムの記録媒体

【特許請求の範囲】

【請求項１】　デジタル情報処理装置を用いて、素体の有限次元拡大体の元として表現された暗号を復号する方法において、前記暗号に第１の秘密鍵を乗算するステップと、第２の秘密鍵で暗号内での要素の順序を置換してメッセージ対応部とノイズとに分離するステップ、とを有することを特徴とする、復号方法。

【請求項２】　第１の秘密鍵を、前記有限次元拡大体の原始多項式の原始根のべき乗とすることを特徴とする、請求項１の復号方法。

【請求項３】　第２の秘密鍵で分離したメッセージ対応部に、第３の秘密鍵の多項式を乗算することを特徴とする、請求項１または２の復号方法。

【請求項４】　第４の秘密鍵を用いてべき乗根を求めるステップを付加したことを特徴とする、請求項３の復号方法。

【請求項５】　デジタル情報処理装置で、素体の有限次元拡大体の元として表現された暗号を復号するために、情報ネットワークを介して、前記暗号に第１の秘密鍵を乗算するステップと、第２の秘密鍵で暗号内での要素の順序を置換してメッセージ対応部とノイズとに分離するステップとを実行させるためのプログラムを、前記デジタル情報処理装置に送信して、該デジタル情報処理装置で暗号を復号させることを特徴とする、復号方法。

【請求項６】　素体の有限次元拡大体の元として表現された暗号を復号するために、前記暗号に第１の秘密鍵を乗算するための乗算手段と、第２の秘密鍵で暗号内での要素の順序を置換してメッセージ対応部とノイズとに分離するための置換手段、とを備えた復号装置。

【請求項７】　前記乗算手段を、前記有限次元拡大体の原始多項式の原始根のべき乗を暗号に乗算するように構成すると共に、前記置換手段で分離したメッセージ対応部に、第３の秘密鍵の多項式を乗算しかつ第４の秘密鍵を用いてべき乗根を求めるための手段を設けたことを特徴とする、請求項６の復号装置。

【請求項８】　素体の有限次元拡大体の元として表現された暗号を復号するために、前記暗号に第１の秘密鍵を乗算するステップと、第２の秘密鍵で暗号内で

の要素の順序を置換してメッセージ対応部とノイズとに分離するステップとを、デジタル情報処理装置に実行させるためのプログラムを記憶した、デジタル情報処理装置で読み出し可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の利用分野】

この発明は暗号システムや暗号通信に関し、特に多変数の多項式の求解困難性を利用した暗号システムや暗号通信に関する。

【０００２】

【従来技術】

多変数の多項式を用いた暗号が提案されている(例えば、 Matsumoto et al, Public Quadatic Polynomial - tuples for Efficient Signature Verification and Message-encryption, Proc. of EUROCRYPT 88, Springer Verlag, Vol.20, P.P.419-453)。このような暗号では、ガロワ体の元を多項式で表現し、多項式の各次元の係数に、メッセージをコーディングする。そしてメッセージの各要素を変数と見なすと、前記の係数は多変数の多項式となる。しかしながら多変数の多項式を用いた暗号の安全性は確認されておらず、発明者は多変数多項式を用いた暗号の安全性を高めることを検討して、この発明に到った。

【０００３】

【発明の課題】

この発明の基本的課題は、多変数多項式を用いた強固な暗号技術を提供して、これを復号できるようにすることにある(請求項１～８)。

請求項２～４の発明の追加の課題は、復号化の具体的な方法を提供することにある。

請求項５の発明の追加の課題は、情報ネットワークを介して、復号プログラムを配信し、容易に暗号通信を行えるようにすることにある。

請求項６，７の発明の追加の課題は復号装置を提供することにあり、特に請求項７の発明の課題は復号装置の具体的な構成を提供することにある。

請求項８の発明の追加の課題は、復号プログラムを記憶した媒体を提供することにある。

【０００４】

【発明の構成】

この発明は、デジタル情報処理装置を用いて、素体の有限次元拡大体の元として表現された暗号を復号する方法において、前記暗号に第１の秘密鍵を乗算するステップと、第２の秘密鍵で暗号内での要素の順序を置換してメッセージ対応部とノイズとに分離するステップ、とを有することを特徴とする（請求項１）。デジタル情報処理装置には、コンピュータの他に、暗号化や復号のための論理回路を組み込んだチップなどが含まれる。この発明で復号すべき暗号は、素体の有限次元拡大体の元であり、多項式表現での各次元の係数などに、メッセージの各要素が多変数多項式としてコーディングされたものである（請求項１～８）。

【０００５】

好ましくは、第１の秘密鍵を、前記有限次元拡大体の原始多項式の原始根のべき乗とする。

また好ましくは、第２の秘密鍵で分離したメッセージ対応部に第３の秘密鍵の多項式を乗算する。

最も好ましくは、第３の秘密鍵の多項式の乗算しかつ第４の秘密鍵を用いてべき乗根を求める。多項式の乗算とべき乗根を求める順序はどちらが先でも良いが、好ましくは先に多項式を乗算し、次いでべき乗根を求める。

【０００６】

またこの発明は、デジタル情報処理装置で、素体の有限次元拡大体の元として表現された暗号を復号するために、情報ネットワークを介して、前記暗号に第１の秘密鍵を乗算するステップと、第２の秘密鍵で暗号内での要素の順序を置換してメッセージ対応部とノイズとに分離するステップ、とを実行させるためのプログラムを、前記デジタル情報処理装置に送信して、該デジタル情報処理装置で暗号を復号させる復号方法にある（請求項５）。

この復号方法では最も好ましくは、第１の秘密鍵を、前記有限次元拡大体の原始多項式の原始根のべき乗とし、第２の秘密鍵で分離したメッセージ対応部に第

３の秘密鍵の多項式を乗算し、第３の秘密鍵の多項式の乗算しかつ第４の秘密鍵でべき乗根を求めて復号する。

【０００７】

またこの発明は、素体の有限次元拡大体の元として表現された暗号を復号するために、前記暗号に第１の秘密鍵を乗算するための乗算手段と、第２の秘密鍵で暗号内での要素の順序を置換してメッセージ対応部とノイズとに分離するための置換手段、とを備えた復号装置にある（請求項６）。

好ましくは、前記乗算手段を、前記有限次元拡大体の原始多項式の原始根のべき乗を暗号に乗算するように構成すると共に、前記置換手段で分離したメッセージ対応部に、第３の秘密鍵の多項式を乗算しかつ第４の秘密鍵でべき乗根を求めるための手段を設ける。

【０００８】

またこの発明は、素体の有限次元拡大体の元として表現された暗号を復号するために、前記暗号に第１の秘密鍵を乗算するステップと、第２の秘密鍵で暗号内での要素の順序を置換してメッセージ対応部とノイズとに分離するステップとを、デジタル情報処理装置に実行させるためのプログラムを記憶した、デジタル情報処理装置で読み出し可能な記録媒体にある（請求項８）。

【０００９】

【発明の作用と効果】

発明者は、素体の有限次元拡大体上の多変数多項式を用いた、新規な暗号技術を開発した。この暗号技術では例えば、

1)　メッセージと多項式とを乗算して多項式の係数にメッセージの各要素をコーディングすること、

2)　メッセージにノイズを付加して対称群の元を作用させノイズとメッセージとをシャッフルすること、

3)　メッセージに有限次元拡大体の元を乗算すること、

の３つの要素を用いる。そして実用的には少なくとも、メッセージにノイズを付加して置換群（対称群）の元を作用させた後、メッセージに拡大体の元を乗算して、拡大体の元の多項式表現での各次元にメッセージとノイズとを混合してコー

ディングすればよい。上記の暗号化を実際に行うには、暗号化のアルゴリズムを伏せて、単に暗号の各要素をメッセージの多項式と見なして、メッセージの値を上記の多項式に代入すればよい。このようにして得られた暗号は強度が高い。例えば、有限次元拡大体上でメッセージに多項式を乗算して、拡大体の元を多項式表現すると、各次元の係数はメッセージの複数の要素が入り交じった多変数の多項式となる。しかしながら、多項式とメッセージとの乗算のみでは、暗号の安全性は確認されていない。

【００１０】

上記の多変数多項式の暗号に、ノイズの付加とノイズとメッセージとのシャッフルとを加えると、暗号を破ることは著しく困難となる。さらに、ノイズとメッセージとのシャッフルの後に、拡大体の元の乗算等を加えると、暗号を破るのはさらに困難になる。このようにして、強度が改善された暗号システムが得られる。この暗号システムでは、暗号化の過程では、暗号システムの特徴は余り表れない。暗号を復号する過程で、暗号化のアルゴリズムに対応した処理が表れ、復号に必要な処理は暗号化の処理の裏返しである。そこで上記の暗号システムを実用化するには、復号方法や復号装置等を提供する必要がある。

【００１１】

この発明では、メッセージを素体の有限次元拡大体の元と見なす。以下では、有限次元拡大体を拡大体、あるいは単に体と呼ぶことがある。そしてメッセージを多項式の不定元に代入した暗号に対して、第１の秘密鍵（有限次元拡大体の元）の乗算と、第２の秘密鍵での暗号内の要素の置換による、メッセージ対応部とノイズとの分離を行う（請求項１）。この暗号を破るには、第１の秘密鍵と第２の秘密鍵が必要で、いずれも秘密鍵の候補は極めて多く、かつ第１の秘密鍵での乗算には有限次元拡大体を生成した既約多項式等を知る必要がある。この発明では、安全な暗号システムが得られる(請求項１～８)。

【００１２】

請求項２の発明では、第１の秘密鍵を前記有限次元拡大体の原始多項式の原始根のべき乗とする。このため第１の秘密鍵は、べきの値を変えることにより、極めて広い範囲から選ぶことでができ、安全性が高い。また原始根のべき乗は乗算

が簡単で、復号が容易である。

【００１３】

請求項３の発明では、第２の秘密鍵で分離したメッセージ対応部に、第３の秘密鍵の多項式を乗算する。復号には、第１の秘密鍵との乗算、第２の秘密鍵での置換操作、第３の秘密鍵の多項式との乗算が必要で、仮に第３の秘密鍵を入手しても、ノイズを除いた有限次元拡大体の生成に用いた既約多項式等を知らなければ多項式との乗算ができず、暗号の信頼性が極めて高い。

【００１４】

請求項４の発明では、第３の秘密鍵の多項式の乗算しかつ第４の秘密鍵でべき乗根を求める。復号には、第１の秘密鍵との乗算、第２の秘密鍵での置換操作、第３の秘密鍵の多項式との乗算、べきの乗数等を示す第４の秘密鍵でべき乗根を求めることが必要で、第４の秘密鍵を知らなければ、メッセージの各要素の複雑な多項式等の段階までしか暗号を破れないため、暗号の信頼性はさらに高い。

【００１５】

請求項５の発明では、復号プログラムを情報ネットワークを介してデジタル情報処理装置に送信し、送信した復号プログラムで復号する。このため、復号プログラムの配布が容易になる。

【００１６】

請求項６～８の発明では、この発明に適した復号装置や復号プログラムの記録媒体を提供し、特に請求項７の発明では、強固に暗号化した暗号をデコードできるので、暗号システムの安全性が特に高い。

【００１７】

以上のように、この発明では新規な暗号化技術を元にして、それに対応した復号方法や復号装置等を提供するので、信頼性の高い暗号システムを構築できる。

【００１８】

【実施例】

図１～図６に実施例を示す。予め主な記号を説明すると、ＧＦ(2^k)、ＧＦ(2^n)はガロワ体を表す。用いる体の素体としては標数ｐ（ｐは素数)のガロワ体の他に、標数が０の体、即ち有理数体Ｑ等でも良い。標数ｐは素数あるいは０とする

が、デジタル情報処理装置での処理の便宜のために、２が好ましい。ガロワ体ＧＦ(2^k)、ＧＦ(2^n)は素体の有限次元拡大体の例で、ｋの値は例えば６４～１６３８４程度とし、実施例では１０２４を想定する。ｎの値は例えば２ｋ程度とし、１２８～３２７６８程度として、実施例では２０４８を想定する。

【００１９】

Ｆ(Ｘ)はガロワ体ＧＦ(2^k)の原始多項式で、ｋ次の多項式であり、同様にＨ(Ｘ)はガロワ体ＧＦ(2^n)の原始多項式で、ｎ次の多項式であり、復号を容易に行うため、Ｆ(Ｘ)やＨ(Ｘ)は原始多項式が好ましい。しかしＦ(Ｘ)はガロワ体ＧＦ(2^k)の単なる既約多項式でもよく、同様にＨ(Ｘ)はガロワ体ＧＦ(2^n)の単なる既約多項式でも良い。αは多項式Ｆ(Ｘ)の根の１つであり、　Ｆ(α)＝０　となる。γはＨ(Ｘ)の原始根の１つで、　Ｈ(γ)＝０　であり、ｘは自然数で、γ^xはガロワ体ＧＦ(2^n)の０でない元である。

【００２０】

Ｍはメッセージを意味し、実施例では１０２４ビット長のデータで、１０２４個の要素ｍ１～ｍｋ（例えばｋ＝１０２４）からなるベクトルと見なすことができ、ガロワ体ＧＦ(2^k)の元である。この明細書で、自然数の集合Ｎは０及び正の整数の集合とする。暗号化のアルゴリズムでは、ｔ個の多項式、(いずれもガロワ体ＧＦ(2^k)の元)、β１(α)，β２(α)，…，βｔ(α)を用い、

Ｍ(α)＝Ｍβ１(α)・Ｍβ２(α)・…・Ｍβｔ(α)　mod　Ｆ(α)　　(1)

に従って、メッセージＭを第１段の暗号Ｍ(α)に変換する。Ｍ(α)を、メッセージ対応部と呼ぶ。またβ１(α)～βｔ(α)の積を単にβと呼ぶ。式(１)等の演算はガロワ体上の演算であり、Ｆ(α)での剰余を問題にしていることは明らかなので、文脈から明らかな場合、剰余演算を行っていることを明記しない場合がある。

【００２１】

ｎ－ｋ次元(例えば１０２４次元で、実施例では１０２４ビット長)のノイズｒ(α)を用意し、メッセージ対応部Ｍ(α)の末尾などに付加し、これに対称群（置換群）の元を作用させて、メッセージ対応部Ｍ(α)の各要素とノイズｒ(α)の各要素の順序を置換し、要素を互いにシャッフルしたものをΓとする。Γはｎ次元のデータで、ガロワ体ＧＦ(2^n)の元である。Ｍ(α)からΓへの写像を$\Phi^{-1}nk$、

復号時に使用するΦ^{-1}nkの逆写像をΦnkとする。M(α)とΓとの間の変換を、暗号化か復号かを区別せずに、置換と呼び、暗号化を意味するか、復号を意味するかは、文脈により指定する。

【００２２】

Γにγ^{x}を乗算すると、得られる多項式Ｃの各次元の係数は、ノイズに由来するものとメッセージに由来するものとが入り交じった多項式となる。多項式Ｃを各次元の要素Ｃｉの集合として表記すると　Ｃ＝｛Ｃｉ(Ｍ)｝　となる。このＣが暗号で、メッセージＭの関数であることを強調する場合、暗号ＣをＣ(Ｍ)と表記する。

【００２３】

以上に暗号化のアルゴリズムを示したが、暗号化は実用的にはアルゴリズムを伏してより簡便に行う。公開鍵として、Ｃ(Ｘ)＝｛Ｃｉ(Ｘ)｝を公開し、公開鍵のＸにＭを代入すると、メッセージＭの各要素（ｍ1～ｍk）の多変数の多項式として各Ｃｉ(Ｍ)が定まり、これを暗号とする。

【００２４】

秘密鍵は、Ｆ(Ｘ)，Ｈ(Ｘ)，ｘ(あるいはγ^{x})，Φnk，β，ｔで

$$\beta=\beta 1(\alpha)\cdot\beta 2(\alpha)\cdot\cdots\cdot\beta t(\alpha) \qquad (2)$$

で、ｔは１以上の自然数である。γが原始根の場合、ガロワ体ＧＦ(2^{n})の任意の０でない元は、γ^{-x}と表現でき、原始根のべき乗との乗算は容易である。ｆはM^{t}からべき乗根Ｍを求めるための自然数（乗数）で、ｔが$2^{k}-1$と素なら、このようなｆが存在する。このことから、(ｔ，$2^{k}-1$)は１が好ましい。なお(ａ，ｂ)は、ａ，ｂの最大公約数を意味する記号である。

【００２５】

以下で、ネットワークは情報ネットワークを意味するものとし、デジタル情報処理装置はコンピュータや、論理回路を内蔵した暗号通信用のチップ等を意味するものとする。記録媒体は、コンピュータや復号用のチップ等で読み取り可能なものとする。

【００２６】

図１に、暗号化装置４と復号装置６との接続を示すと、これらはインターネッ

ト等のネットワークにより接続され、暗号化装置４は、復号装置６側に設けた公開鍵記憶部８から、公開鍵Ｃ(Ｘ)を入手して、平分作成部２で作成したメッセージＭを暗号化する。メッセージＭはガロワ体ＧＦ(2^k)の元である。メッセージＭの構成は(m1，m2，…，mk)で、ｋビット長であり、公開鍵Ｃ(Ｘ)を用いた暗号Ｃ(Ｍ)への暗号化では、ｎ次元の公開鍵Ｃ(Ｘ)の各要素Ｃｉ(Ｘ)に対して（ｉ＝１～ｎ）、Ｘにメッセージを代入する。この結果、得られる暗号Ｃ(Ｍ)はガロワ体ＧＦ(2^n)の元となる。

【００２７】

復号装置６側には秘密鍵記憶部１０があり、ガロワ体ＧＦ(2^k)の原始多項式Ｆ(Ｘ)，ガロワ体ＧＦ(2^n)の原始多項式Ｈ(Ｘ)，ガロワ体ＧＦ(2^n)の原始根γの値（原始根が複数ある場合）と、そのべき乗γ^xのｘ，ノイズとメッセージ対応部とを分離するための対称群の元Φnk，メッセージＭをガロワ体ＧＦ(2^k)内で多項式と乗算した際の多項式β，並びに多項式βとの乗算に伴いメッセージＭをｔ乗した際のｔ等が記憶されている。

【００２８】

１２は乗算処理部で、暗号Ｃ(Ｍ)にガロワ体ＧＦ(2^n)の元γ^{-x}を乗算し、Γに変換する。１４は置換処理部で、Γに対称群の元Φnkを作用させ、メッセージ対応部Ｍ(α)とノイズとに分離し、メッセージ対応部Ｍ(α)を取り出す。１６は第２の乗算処理部で、メッセージ対応部Ｍ(α)に、多項式βの逆元β^{-1}を乗算し、メッセージＭのｔ乗を求める。そしてメッセージＭのｔ乗に対して、適宜の自然数ｆでべき乗して、メッセージＭに復号する。このようなｆは、ｔが2^k-1と素であれば存在する。

【００２９】

図２に、暗号化のアルゴリズムを示す。メッセージＭ、(例えば１０２４ビット長のデータで、メッセージＭ内に既にノイズを含んでいても良い)、をガロワ体ＧＦ(2^k)の元とし、式(1)

$$M(\alpha)=M\beta 1(\alpha)\cdot M\beta 2(\alpha)\cdot\cdots\cdot M\beta t(\alpha) \mod F(\alpha) \qquad (1)$$

により処理して、メッセージ対応部Ｍ(α)とする。メッセージ対応部Ｍ(α)をｋ－１次以下の多項式と見なすと、各係数にはメッセージＭの各要素ｍ1～ｍkが複

雑に入り交じり、ｍ1～ｍkのｔ次の多項式と見なすことができる。メッセージ対応部Ｍ(α)を単独で用いた場合の暗号の信頼性は確認されておらず、以下の手続きで暗号を補強する。

【００３０】

メッセージ対応部Ｍ(α)をｎ－ｋ次元のノイズｒ(α)とシャッフルする。このシャッフルは、例えばメッセージ対応部Ｍ(α)の末尾にノイズｒ(α)を付加し、これに対称群の元Φ^{-1}nkを作用させて、ガロワ体ＧＦ(2^n)の元Γに変換するものである。

【００３１】

続いてΓにγ^xを乗算し、ノイズｒ(α)の各成分とメッセージ対応部Ｍ(α)の成分を、ガロワ体ＧＦ(2^n)での多項式表現の各次数において、複雑に入り交じらせる。ここにγは原始多項式Ｈ(Ｘ)の原始根で、ｘの値を選ぶことにより、ガロワ体ＧＦ(2^n)の０以外の任意の元を、γ^xとして表現することができる。この結果、得られた暗号Ｃは極めて強固なものとなる。

【００３２】

なおここで暗号化には，式(1)による処理と、ノイズｒ(α)の付加と置換（シャッフル）、並びにγ^xの乗算の３段階の手続きを行ったが、これらはこの順に行う必要はない。例えば最初にメッセージＭとノイズｒとのシャッフルを行った後に、多項式との乗算や原始根のべき乗との乗算を行っても良く、あるいは最初に原始根のべき乗との乗算を行った後に、ノイズとのシャッフルを行い、最後に多項式との乗算を行っても良い。また実施例での暗号の信頼性は極めて高いので、上記の３手続きに代えて、ノイズの付加並びにシャッフル、及び多項式との乗算もしくは原始根のべき乗との乗算のいずれか一方を行っても良い。

【００３３】

暗号化のアルゴリズムを図２に示したが、実際の暗号化では送信者に暗号化のアルゴリズムを知らせる必要はない。実際の暗号化では、図３に示すように、公開鍵Ｃ(Ｘ)として、メッセージＭと同じ長さの不定元Ｘを用い、Ｘの多項式として公開鍵の各要素Ｃｉ(Ｘ)（ｉ＝１～ｎ）を公開する。送信者は、不定元Ｘにメッセージを代入すれば、暗号Ｃ(Ｍ)が得られる。従って暗号化は極めて容易で

あり、かつ公開鍵Ｃ(Ｘ)は強い１方向性の関数である。

【００３４】

図４に復号のアルゴリズムを示す。復号装置６で受信した暗号Ｃ(Ｍ)に対し、γ^{-x}を乗算し、Γを求める。γ^{-x}はガロワ体ＧＦ(2^n)の元であり、この乗算は容易である。次いでΓにノイズの付加と置換とに用いた写像$\Phi^{-1}nk$の逆置換から成る写像Φnkを施し、Γをメッセージ対応部Ｍ(α)へと変換し、ノイズｒ(α)を除去する。この過程で、ガロワ群の元の数は2^nから2^kへと減少する。続いてメッセージ対応部Ｍ(α)に対して、式(1)で用いたｔ個の多項式β1(α)～βｔ(α)の積βの逆元を乗算し、Ｍ(α)をM^tに変換する。ここでｔと2^k-1とが素であれば、適当な自然数ｆが存在して、$M^{tf}=M$となり、これからメッセージＭを求めることができる。

【００３５】

図５に、復号プログラムのネットワーク２４を介しての配布を示す。２０は配信者で２２は、受信者で、例えば適当な秘密鍵等を用いて、受信者２２は配信者２０に対して復号プログラムの送信を要求し、これに対応してネットワーク２４を介して復号プログラムを配布する。配布送信する復号プログラムは、図４のアルゴリズムを実現したものである。

【００３６】

図６に、暗号装置３０の例を示すと、３２は入出力で、外部との通信や外部のコンピュータ等との接続に用い、３４は公開鍵記憶部で、公開鍵Ｃ(Ｘ)を記憶して公開し、３６は乗算処理部でγ^{-x}を乗算し、γ^{-x}の値は乗算処理部３６で記憶しているものとする。３８は置換処理部で、Γをメッセージ対応部Ｍ(α)へ変換するための対称群の元を記憶して、ΓをＭ(α)に変換し、４０は乗算処理部で、多項式β^{-1}を記憶して、メッセージ対応部Ｍ(α)をM^tと乗算する。４２はｆ乗処理部で、M^tをさらにｆ乗して、メッセージＭへと復号する。４４は暗号化部で、暗号装置３０側で作成したメッセージＭを暗号化するためのものである。なおこれらの処理部３６～４４は、レジスタと論理ゲート等の組み合わせ等により容易に実現でき、あるいはまたソフトウエアをコンピュータに搭載しても実現できる。

【００３７】

実施例は公開鍵暗号として用いる場合を示したが、秘密鍵暗号として用いても良く、その場合、秘密鍵の原始多項式やｘの値、ノイズとのシャッフルに用いた対称群の要素Φnk、多項式β、ｔの値、あるいはMの長さ等を適宜に更新すれば、極めて寿命の長い暗号システムが得られる。実施例は特定の処理を示したが、これらと等価な処理はこの発明に含まれ、例えば各秘密鍵は文字通りに秘密鍵を記憶する必要はなく、秘密鍵と等価、もしくは秘密鍵に変換可能なものであればよい。

【図面の簡単な説明】

【図１】　実施例での暗号化装置と復号装置との接続を示すブロック図

【図２】　実施例での暗号化アルゴリズムを示すフローチャート

【図３】　実施例での暗号化処理を示すフローチャート

【図４】　変形例での復号アルゴリズムを示すフローチャート

【図５】　実施例での復号プログラムの配信を示す図

【図６】　実施例での復号装置の構成を示すブロック図

【符号の説明】

２　　平分作成部

４　　暗号化装置

６　　復号装置

８　　公開鍵記憶部

１０　　秘密鍵記憶部

１２　　乗算処理部

１４　　置換処理部

１６　　乗算処理部

２０　　配信者

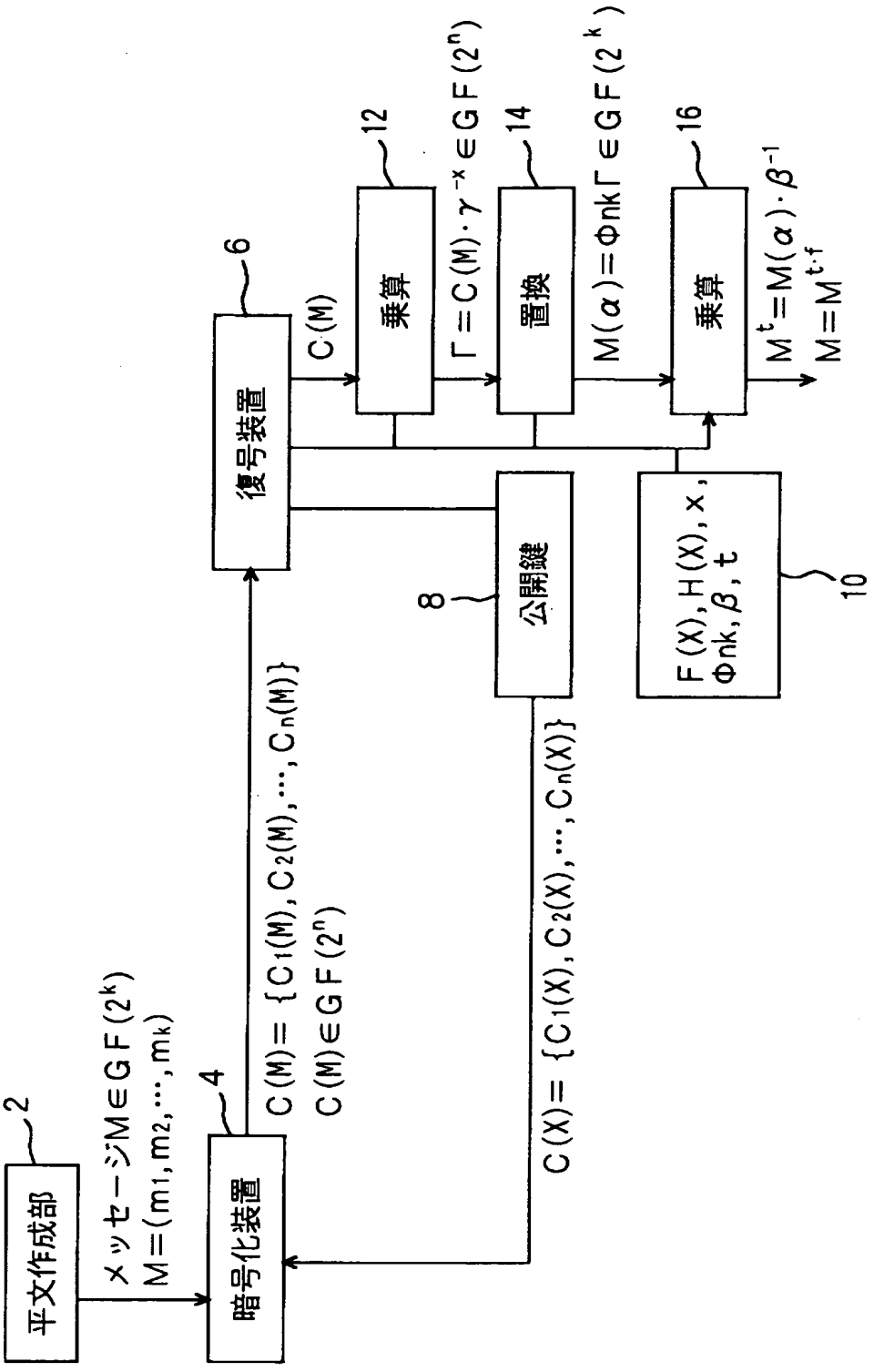
２２　　受信者

２４　　ネットワーク

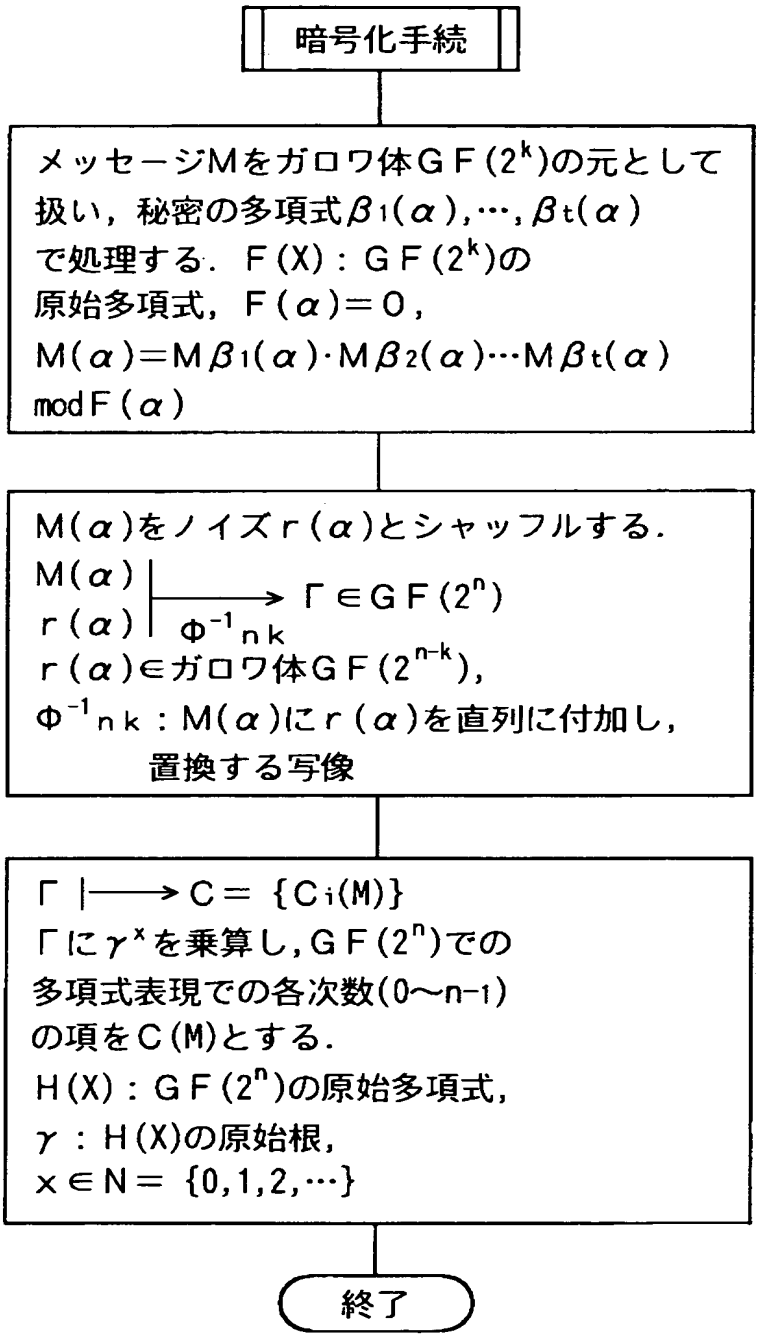
３０	暗号装置
３２	入出力
４４	暗号化部
３６	乗算処理部
３８	置換処理部
４０	乗算処理部
４２	ｆ乗処理部
４４	暗号化部

【書類名】図面

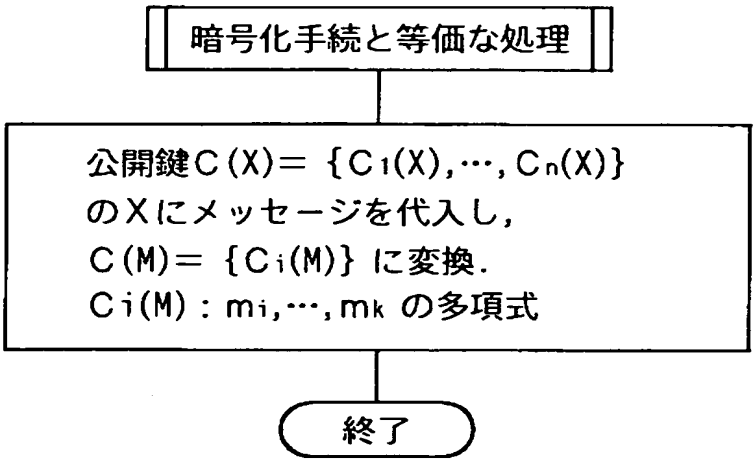
【図１】


平文作成部
2
メッセージ M∈GF(2^k)
M=(m1, m2, ···, mk)
暗号化装置
4
C(M)={C1(M), C2(M), ···, Cn(M)}
C(M)∈GF(2^n)
復号装置
6
C(M)
乗算
12
Γ=C(M)·γ^-x ∈GF(2^n)
置換
14
M(α)=ΦnkΓ∈GF(2^k)
乗算
16
M^t=M(α)·β^-1
M=M^t·f
公開鍵
8
C(X)={C1(X), C2(X), ···, Cn(X)}
F(X), H(X), x,
Φnk, β, t
10

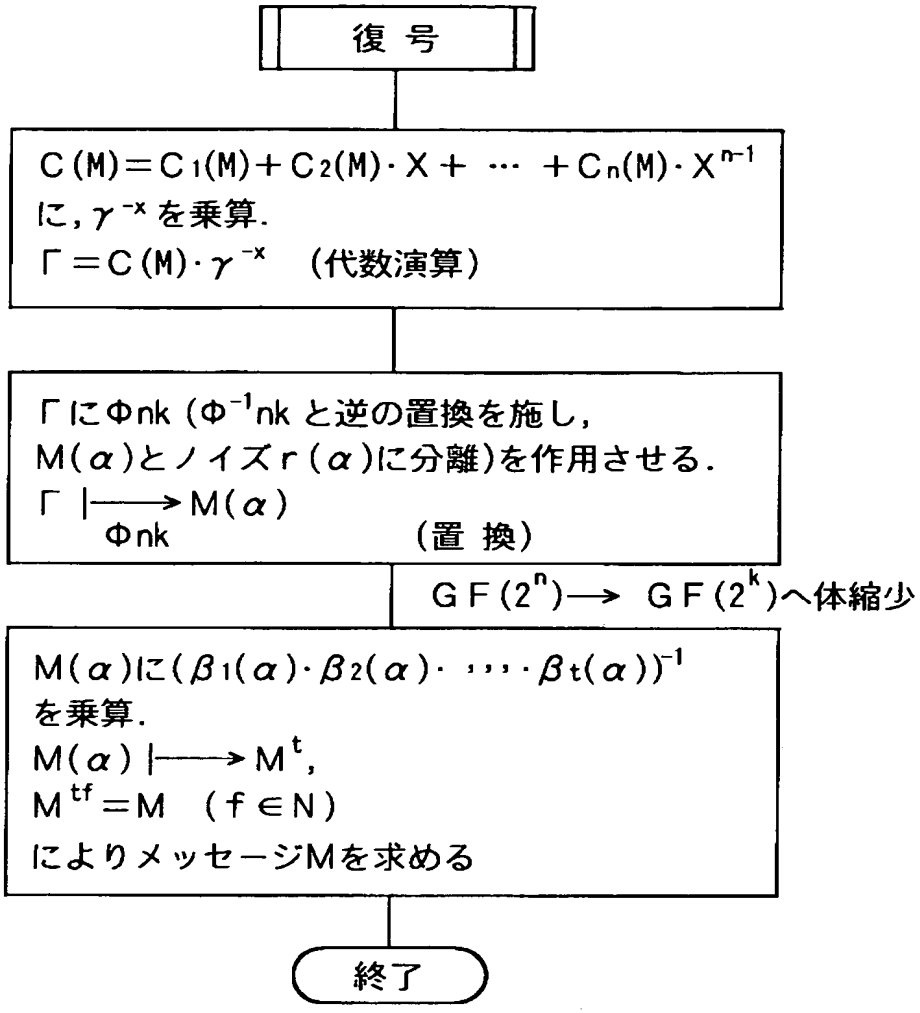
【図２】


暗号化手続
メッセージMをガロワ体ＧＦ(2^k)の元として
扱い，秘密の多項式β1(α),…,βt(α)
で処理する．Ｆ(X)：ＧＦ(2^k)の
原始多項式，Ｆ(α)＝０，
M(α)＝Mβ1(α)･Mβ2(α)…Mβt(α)
modＦ(α)
M(α)をノイズｒ(α)とシャッフルする．
M(α)
r(α)
Φ^-1 nk
Γ∈ＧＦ(2^n)
r(α)∈ガロワ体ＧＦ(2^n-k),
Φ^-1 nk：M(α)にｒ(α)を直列に付加し，
置換する写像
Γ ⟶ C＝ {Ci(M)}
Γにγ^xを乗算し，ＧＦ(2^n)での
多項式表現での各次数(0～n-1)
の項をＣ(M)とする．
Ｈ(X)：ＧＦ(2^n)の原始多項式，
γ：Ｈ(X)の原始根，
x∈Ｎ＝ {0,1,2,…}
終了

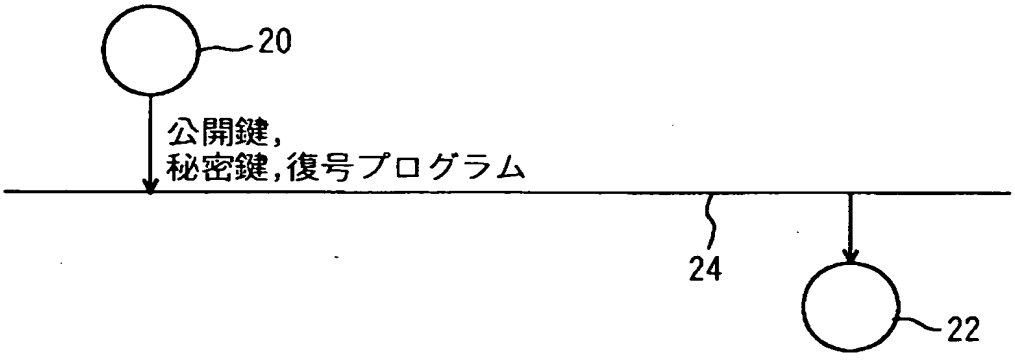
【図３】


暗号化手続と等価な処理
公開鍵C(X)＝ {C1(X),…, Cn(X)}
のXにメッセージを代入し,
C(M)＝ {Ci(M)} に変換.
Ci(M)：mi,…, mk の多項式
終了

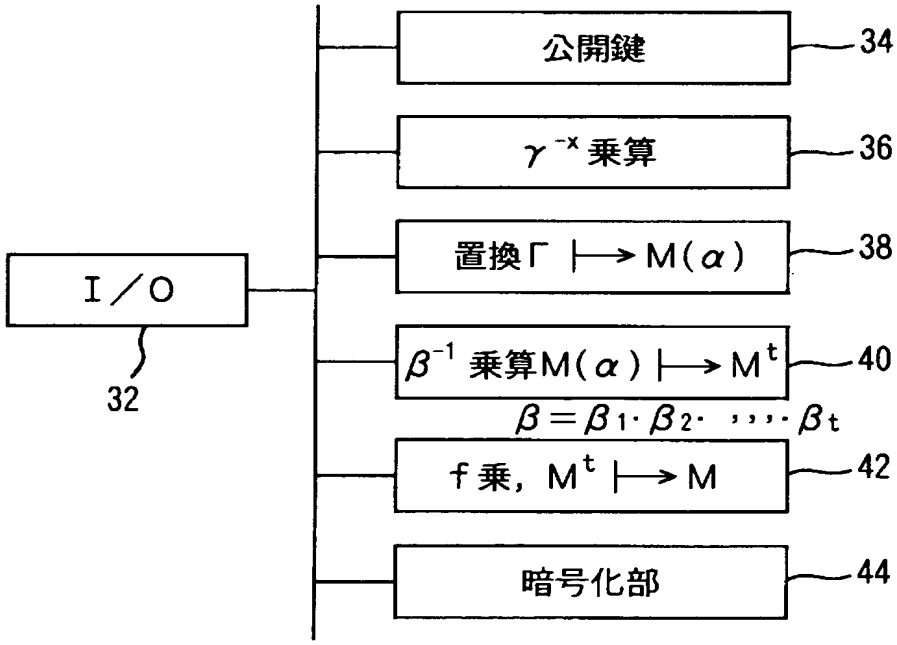
【図４】


復 号
C(M)＝C1(M)＋C2(M)・X＋ … ＋Cn(M)・X^n-1
に，γ^-x を乗算.
Γ＝C(M)・γ^-x （代数演算）
ΓにΦnk (Φ^-1nk と逆の置換を施し，
M(α)とノイズr(α)に分離)を作用させる.
Γ |⟶ M(α)
Φnk （置 換）
GF(2^n)⟶ GF(2^k)へ体縮少
M(α)に(β1(α)・β2(α)・ ,,,・βt(α))^-1
を乗算.
M(α) |⟶ M^t,
M^tf＝M （f∈N）
によりメッセージMを求める
終了

【図５】


20
公開鍵，
秘密鍵，復号プログラム
24
22

【図６】


公開鍵
34
γ^-x 乗算
36
置換Γ ⟼ M(α)
38
I／O
β^-1 乗算M(α) ⟼ M^t
40
β＝β1・β2・ ，，，・βt
f 乗，M^t ⟼ M
42
暗号化部
44
32
30

【書類名】　　要約書

【要約】

【構成】　メッセージＭをガロワ体ＧＦ(2^k)の元(ｍ１，ｍ２，…，ｍｋ)と見なして、Ｍに多項式$\beta 1(\alpha)$～$\beta t(\alpha)$を乗算し、

$M(\alpha)=M\beta 1(\alpha)\cdot M\beta 2(\alpha)\cdot\cdots\cdot M\beta t(\alpha)$

を求める。Ｍ(α)に直列にｎ－ｋ次のノイズベクトルｒ(α)を付加して、ｎ次元に拡張し、置換操作を施して、Γに変換する。Γにガロワ体ＧＦ(2^n)の元γ^x(γはガロワ体ＧＦ(2^n)の乗法群の原始根)を乗算し、暗号Ｃ(Ｍ)とする。実用的には暗号Ｃ(Ｍ)は、公開鍵Ｃ(Ｘ)のＸにメッセージＭを代入することで求められる。暗号Ｃ(Ｍ)にγ^{-x}を乗算し、逆の置換操作を施して、ノイズベクトルｒ(α)を分離し、$\beta 1(\alpha)$～$\beta t(\alpha)$の逆元を乗算し、適当にべき乗してＭに復号する。

【効果】　多変数の多項式を用いた強固な暗号システムを提供できる。

【選択図】　　図１

認定・付加情報

特許出願の番号	特願２０００－０６６２２６
受付番号	５００００２８６０５２
書類名	特許願
担当官	第八担当上席　００９７
作成日	平成１２年　４月２０日

＜認定情報・付加情報＞

【提出日】　平成12年 3月10日

次頁無

出　願　人　履　歴　情　報

識別番号　　〔０００００６２９７〕

１．変更年月日　　１９９０年　８月　７日
〔変更理由〕　新規登録
住　所　京都府京都市南区吉祥院南落合町３番地
氏　名　村田機械株式会社

出　願　人　履　歴　情　報

識別番号　　〔５９７００８６３６〕

１．変更年月日　　１９９７年　１月２１日
［変更理由］　新規登録
住　所　　大阪府箕面市粟生外院４丁目１５番３号
氏　名　　笠原　正雄